Security Software
for
Servers and Workstations

The candidates:

   Symantec -- Symantec Enterprise Security Manager

   Bindview – Internet Security

   NetIQ - Security Analyzer

All the candidates have very similar features or add on:

   Testing Criteria:

      Ease of Use:
      Update Ability:
      Sales and Tech Support:
      Security Checks:

   When testing a product, it is always interesting to install the product before talking to the sales representatives. This give a person the chance to see what really works and what the sales person is going to say. I asked many of the sales staff how their product could be lesser, equal or greater than their competitor. I feel this is a good test to see if they know their product as well as the competition.

   I found Symantec have a high ego of themselves. Symantec did not know their competition as well because they were looking for sales. NetIQ and Bindview new each others products well enough to be able to give me a clear and concise view of each of their products. Bindview admitted that NetIQ had a better look for security on the server. NetIQ admitted that Bindview had a better intrusion detection system.

The following criteria was used.

Ease of Use:

From my findings Bindview and NetIQ had software that was easy to understand and is only a two tier system. The installation was a one step process. The Symantec version was a bit more complicated and consisted of a three tier system. A tier is a process of steps, for example NetIQ and Bindview only need a server to scan other servers where as Symantec needs a Server to talk to smaller servers that gather information.

Update Ability:

Symantec and NetIQ have a system that will auto update as needed. It can be scheduled or on demand from the corporation. Bindview had a confusing way of authenticating through an email server to allow the download to be given to the user.

Sales and Tech Support:

Symantec, Bind view and NetIQ had excellent tech support. The sales staff was great from Bindview and NetIQ. Symantec's sales staff is pushy and does not deal well with the current purchase. Symantec is more worried about sales than the customer.

Security Checks:

All three worked well. I felt that Bindview and NetIQ have the best documentation for supporting the reason for the security change. In addition to the security change, Bind view and NetIQ helped out in descriptive documentation for making the resolution to the individual servers.

I am recommending NetIQ:

1) Helpful Tech Support
2) Ease of use
3) Update ability with a few clicks
4) Security Checks are comparable to other software vendors
5) Expandability for
    A) File and Storage Administrator - The product's straightforward interface and extensive, flexible reporting features simplify tasks, such as determining who can access your file

system, eliminating and preventing enterprise security holes and reporting on storage utilization.

B) Exchange Administrator - Exchange Administrator lets you define policies that are automatically enforced and propagated across all directories, mailboxes and distribution lists.

C) Security Manager - Security Manager provides users with real-time security monitoring, host-based intrusion detection, policy-based security configuration management and automated incident response.

Security Manager would be the next step in the NetIQ purchases. This would allow for intrusion detection in real time. I feel this would not be purchased at this time until The Security Analyzer has been implemented.

Please Note!!!

      I don't want to give the impression that this software will be a "Great Wall". This software is like a seat belt in a vehicle. It is only as good if you use it and sometimes nothing will stop injuries from happening anyway.